נציג בית העסק הנכבד,

מסמך זה הינו תרגום שאלון ההערכה העצמית SAQ.

המסמך תורגם מהשפה האנגלית לשפה העברית על מנת לסייע לך במילוי השאלון המקורי.

יודגש כי המסמך המקורי נכתב בשפה האנגלית והוא הנוסח המחייב.

התרגום העברי פונה לנשים וגברים כאחד ונוסח בלשון זכר מטעמי נוחות בלבד.

למרות כל המאמצים והזהירות בתרגום מהשפה האנגלית, חברת EverCompliant ו/או חברות האשראי ; ישראכרט בע"מ, לאומי קארד בע"מ וכ.א.ל בע"מ (להלן: "הארגונים") אינם ערבות לטיב התרגום ו/או דיוקו.

לכן הארגונים לא יישאו בכל אחריות ו/או נזק עקב השימוש במסמך בשפה העברית.

מודגש בזאת כי הנעזר במסמך המתורגם בשפה העברית לצורך מילוי השאלון המקורי עושה זאת על דעתו ועל אחריותו בלבד.

בברכה,

ישראכרט

תעשיית כרטיסי התשלום (PCI)
תקן אבטחת מידע
שאלון הערכה עצמית C (SAQ)
והצהרת תאימות

בתי עסק עם מערכות תשלום המחוברות לאינטרנט, אין שמירה אלקטרונית של נתוני אשראי

גרסה 3.0

פברואר 2014

שינויי מסמך

תאריך	גרסה	תיאור
אוקטובר 2008	1.2	התאמת התוכן לתקן PCI DSS החדש גרסה 1.2 והכנסת שינויים משניים שחלו מאז גרסה 1.1 המקורית
אוקטובר 2010	2.0	התאמת התוכן לדרישות ולנהלי הבדיקה של תקן PCI DSS החדש גרסה 2.0
פברואר 2014	3.0	התאמת התוכן לדרישות ולנהלי הבדיקה של תקן PCI DSS החדש גרסה 3.0 ולשלב אפשרויות תגובה נוספות.

תוכן עניינים

Copyright 2014 PCI Security Standards Council LLC

לפני שמתחילים

שאלון הערכה עצמית C פותח עבור בתי עסק רלוונטיים המעבדים נתוני אשראי באמצעות מערכות תשלום (למשל מערכות תשלום בנקודת מכירה – POS) המחוברות לאינטרנט (באמצעות מודם, DSL וכו').

בתי עסק המתאימים למילוי שאלון C מעבדים נתוני אשראי דרך מערכות נקודות מכירה (POS) או באמצעות מערכות תשלום אחרות המחוברות לאינטרנט, הם אינם שומרים שום נתוני אשראי על אף אחת ממערכות המחשוב, והם עשויים להיות חנויות (המבצעות עסקאות כרטיס נוכח) או עסקים למסחר אלקטרוני או כאלה המבצעים עסקאות בטלפון/דואר (עסקאות כרטיס לא נוכח).

בתי עסק אלו מאשרים את עמידתם בתקן באמצעות מילוי שאלון C, המאמתים כי:

- לארגון שלך יש מערכת תשלום וחיבור לאינטרנט מאותו מכשיר/עמדה ו/או מאותה רשת מקומית (LAN);
- מערכת התשלום/המחשב המחובר לאינטרנט אינם מחוברים לאף מערכת אחרת בארגון (ניתן להשיג זאת באמצעות חלוקת הרשת לסגמנטים ובידודה של מערכת התשלום/המחשב המחובר לאינטרנט מיתר המערכות);
- החנות של בית העסק אינה מחוברת לחניות במיקומים נוספים, וכל רשת מקומית (LAN) היא לחנות בודדת בלבד;
- הארגון שומר רק דוחות נייר או העתקי נייר של קבלות עם נתוני אשראי; ומסמכים אלו אינם מועברים באופן אלקטרוני; בנוסף
- הארגון אינו שומר נתוני אשראי בפורמט אלקטרוני.

אפשרות זו אינה חלה בשום פנים ואופן על בתי עסק המקיימים מסחר עם עמדות מכירה "פנים מול פנים".

כל חלק בשאלון מתמקד בתחום ספציפי של אבטחת המידע, תוך התבססות על הדרישות המפורטות ב*"דרישות ובנהלי הערכת האבטחה של PCI DSS"*. גרסה מקוצרת זו של השאלון כוללת שאלות הנוגעות לסוג מסוים של בתי עסק קטנים, כפי שמוגדר בקריטריוני הסיווג לעיל. אם חלות על הסביבה שלך דרישות PCI DSS שאינן מופיעות בשאלון זה, זו עשויה להיות אינדיקציה לכך ששאלון זה אינו מתאים לסביבת העבודה שלך. בנוסף, עליך לעמוד בכל הדרישות הרלוונטיות של תקן PCI DSS על מנת לקבל סטטוס 'עומד בתקן PCI DSS'.

הערכה עצמית PCI DSS – שלבי ביצוע

1. יש לזהות את שאלון ההערכה העצמית המתאים לסביבת המסחר הספציפית – למידע, עיין במסמך *Self-Assessment Questionnaire Instructions and Guidelines* באתר האינטרנט של PCI SSC.
2. יש לוודא שסביבת המסחר הוערכה כראוי והיא נכללת בקריטריונים של השאלון שבו נעשה שימוש.
3. יש לבצע הערכה של תאימות סביבת העבודה לדרישות PCI DSS.
4. יש למלא את כל החלקים של מסמך זה:
   - פרק 1 (פרק 1 ו-2 של AOC) – פרטי הערכה ותקציר מנהלים.
   - פרק 2 – שאלון הערכה עצמית של PCI DSS (שאלון הערכה עצמית D)
   - פרק 3 (חלקים 3 ו-4 של AOC) – אשרור פרטי הצהרת התאימות ותוכנית פעולה לסטטוס 'לא עומד בתקן' (במידה ורלוונטי)
5. יש להגיש את שאלון ההערכה העצמית ואת הצהרת התאימות, בצירוף כל מסמך נדרש אחר – כגון דוחות סריקה מאת ספק הסריקות המאושר – לחברת כרטיסי האשראי, לחברה המחזיקה במותג האשראי או לכל דורש אחר.

Copyright 2014 PCI Security Standards Council LLC

הבנת שאלון ההערכה העצמית

השאלות המופיעות תחת העמודה "שאלה" בשאלון הערכה עצמית זה מבוססות על דרישות תקן PCI DSS.
משאבים נוספים המספקים הנחיה לדרישות PCI DSS ואופן המילוי של שאלון ההערכה העצמית מצורפים על מנת לסייע לך בתהליך ההערכה. להלן סקירה של חלק ממסמכים אלה:

מסמך	כולל:
PCI DSS *(תקן PCI לאבטחת מידע: דרישות ונהלי הערכת אבטחה)*	• הנחיות לגבי היקף הסקירה • הנחיות לגבי כוונת דרישות PCI DSS • פרטים על נהלי הבדיקה • הנחיות לגבי בקרות מפצות
מסמכי הוראות והנחיות להערכה עצמית	• מידע על כל שאלוני ההערכה העצמית והקריטריונים להכללה • כיצד לקבוע איזה שאלון הערכה מתאים לעסק/לארגון שלך
תקן PCI לאבטחת מידע ותקן אבטחת נתונים של יישומי תשלום: מילון מונחים, קיצורים וראשי תיבות	• תיאורים והגדרות של המונחים שבהם נעשה שימוש בתקן PCI DSS ובשאלוני ההערכה העצמית

משאבים אלה ואחרים מופיעים באתר האינטרנט של מועצת תקני האבטחה הרשמית של PCI (PCI SSC) בכתובת www.pcisecuritystandards.org. ארגונים מתבקשים לעבור על מסמכי PCI DSS ועל מסמכי התמיכה האחרים לפני ביצוע ההערכה.

בדיקות נדרשות

ההוראות המופיעות תחת העמודה "בדיקות נדרשות" מבוססות על נהלי הבדיקה של תקן PCI DSS, ומספקות תיאור מפורט של סוגי פעילויות הבדיקה שיש לערוך על מנת לוודא שהדרישה אכן נענתה. פרטים מלאים על נהלי הבדיקה עבור כל דרישה ניתן למצוא ב-PCI DSS.

מילוי שאלון ההערכה העצמית

בכל שאלה קיימת בחירה בין מספר תגובות המציינות את מצב החברה בנוגע לאותה דרישה. ***יש לבחור תגובה אחת בלבד לכל שאלה.***

בטבלה להלן תיאור של כל תגובה:

תגובה	מתי יש להשתמש בתגובה זו:
כן	הבדיקות הנדרשות בוצעו וכל מרכיבי הדרישה נענו כפי שהוצהר.
כן עם גיליון עבודה של בקרות מפצות	הבדיקות הנדרשות בוצעו והדרישה נענתה בסיוע בקרה מפצה. כל התגובות בעמודה זו מחייבות מילוי גיליון בקרות מפצות (CCW) המופיע בנספח ב' של שאלון ההערכה העצמית. מידע על השימוש בבקרות מפצות והנחיות למילוי גיליון העבודה מופיעים ב-PCI DSS.
לא	חלק ממרכיבי הדרישה או כולם לא נענו, או נמצאים בתהליך של הטמעה ויישום, או שנדרשות בדיקות נוספות לקבלת מידע על קיומן של דרישות אלה.
לא רלוונטי	הדרישה אינה חלה על הסביבה הארגונית הספציפית (ר' *הנחיה בנוגע לחוסר הרלוונטיות של דרישות ספציפיות מסוימות* להלן). כל התגובות בעמודה זו מחייבות הסבר תומך בנספח ג' של שאלון ההערכה העצמית.

Copyright 2014 PCI Security Standards Council LLC

לא נבדק	הדרישה לא עמדה לשיקול בהערכה ולא נבדקה בדרך כלשהי (לדוגמאות לגבי השימוש באפשרות זו, ר' *הבנת ההבדל בין האפשרות 'לא רלוונטי' לאפשרות 'לא נבחן'*). כל התגובות בעמודה זו מחייבות הסבר תומך בנספח ג' של שאלון ההערכה העצמית.

הנחיה בנוגע לחוסר הרלוונטיות של דרישות ספציפיות מסוימות

אף שרוב הארגונים הממלאים את שאלון C יידרשו לאשרר את התאימות שלהם עם כל אחת מדרישות ה PCI DSS, חלק מהארגונים אשר פועלים במודלים עסקיים ספציפיים מאוד, עשויים לגלות שחלק מהדרישות אינן רלוונטיות עבורם.

לדוגמה, לא מצופה מחברה אשר אינה עושה שימוש בטכנולוגיה אלחוטית כלשהי לאשרר תאימות עם דרישות PCI DSS ספציפיות הנוגעות לניהול טכנולוגיות אלחוטיות (דרישות 1.2.3, 2.1.1 ו-4.1.1, לדוגמה) . יש להביא בחשבון שדרישה 11.1 (שימוש בתהליכים לזיהוי נקודות גישה אלחוטיות לא מורשות) חייבת להתמלא גם במידה והארגון אינו עושה שימוש בטכנולוגיות אלחוטיות, היות ומטרת תהליך זה היא לאתר רכיבים זדוניים בלתי מורשים אשר עשויים להיות מותקנים בארגון ללא ידיעת בית העסק.

אם דרישות כלשהן אינן רלוונטיות לסביבת האשראי של החברה יש לבחור באפשרות "לא רלוונטי" עבור אותה דרישה מסוימת, ולמלא את גיליון "הסבר לחוסר רלוונטיות" שבנספח ג' עבור כל בחירה כגון זו.

החרגה משפטית

אם הארגון נתון להגבלה משפטית המונעת ממנו לעמוד בדרישות מסוימות של תקן PCI DSS, יש לסמן את העמודה "לא" עבור דרישות אלה ולמלא את ההצהרה הרלוונטית בחלק 3.

פרק 1 : פרטי ההערכה

הוראות הגשה

על בית העסק למלא מסמך זה כהצהרה על תוצאות ההערכה העצמית של בית העסק ל*דרישות ונהלי האבטחה של תקן אבטחת המידע של תעשיית כרטיסי האשראי* (PCI DSS). השלם את כל החלקים: על בית העסק להבטיח את מילוי כל אחד מהחלקים של שאלון זה על-ידי הצדדים הרלוונטיים. בכל הנוגע לנהלי הדיווח וההגשה של המסמך, יש ליצור קשר עם חברת כרטיסי האשראי (בנק מסחרי) או עם החברה המחזיקה במותג האשראי.

חלק 1. פרטי בית העסק וחברת ההסמכה הרשמית (QSA) **חלק 1א. פרטי בית העסק**			
שם החברה:		שם(ות) מסחרי(ים):	
שם איש קשר:		תפקיד:	
שם גורם ההסמכה הפנימי (אם רלוונטי):		תפקיד:	
טלפון:		דוא"ל:	
כתובת העסק:		עיר:	
מדינה:		מיקוד:	
אתר אינטרנט:			

חלק 1ב. פרטי חברת ההסמכה הרשמית (QSA- אם רלוונטי)			
שם החברה:			
שם הסוקר המוסמך הראשי:		תפקיד:	
טלפון:		דוא"ל:	
כתובת העסק:		עיר:	
מדינה:		מיקוד:	
אתר אינטרנט:			

Copyright 2014 PCI Security Standards Council LLC

חלק 2. תקציר מנהלים

חלק 2א. סוג העסק המסחרי (יש לסמן את כל הרלוונטיים)

☐ קמעונאי ☐ טלקומוניקציה ☐ מרכולים וסופרמרקטים

☐ דלק ☐ מסחר אלקטרוני ☐ הזמנות דואר/טלפון

☐ אחר (אנא פרט):

אלו סוגים של ערוצי תשלום מציע בית העסק?	אלו ערוצי תשלום כלולים בשאלון הערכה עצמית זה?
☐ הזמנות דואר/טלפון	☐ הזמנות דואר/טלפון
☐ מסחר אלקטרוני	☐ מסחר אלקטרוני
☐ נוכחות כרטיס (פנים אל פנים)	☐ נוכחות כרטיס (פנים אל פנים)

הערה: *אם הארגון מציע תהליכים או ערוצי תשלום שאינם נכללים בשאלון הערכה עצמית זה, יש להיוועץ בחברת כרטיסי האשראי או במותג האשראי בנוגע לאשרור ערוצי התשלום האחרים.*

חלק 2ב: תיאור סביבת כרטיסי האשראי

באיזה אופן ועד כמה בית העסק מעבד, מאחסן או משדר פרטי כרטיסי אשראי?	

חלק 2ג: מיקומים

פרט את סוגי המתקנים והאתרים הנכללים בסקר ה-PCI DSS (לדוגמה, חנויות מסחריות, משרדים ארגוניים, מרכזי נתונים, מוקדים טלפוניים וכיו"ב)

סוג המתקן	מיקום(י) המתקן (עיר, מדינה)

חלק 2ד: מערכות תשלום

האם הארגון משתמש במערכת תשלום אחת או יותר? ☐ כן ☐ לא

Copyright 2014 PCI Security Standards Council LLC

ספק את המידע הבא בנוגע למערכות התשלום שבהם נעשה שימוש בארגונך:

שם מערכת התשלום	מספר גרסה	יצרן מערכת התשלום	האם מערכת התשלום מאושרת לתקן PA-DSS?	תאריך תפוגה של אישור PA-DSS (אם רלוונטי)
			☐ כן ☐ לא	
			☐ כן ☐ לא	
			☐ כן ☐ לא	

חלק 2ה: תיאור הסביבה

הצג תיאור ***<u>פרטני</u>*** של הסביבה הנכללת בהערכה זו. *לדוגמה:* • *חיבורים לתוך סביבת נתוני האשראי (CDE) וממנה.* • *רכיבי מערכת קריטיים בתוך סביבת נתוני האשראי, כגון מסופי נקודות מכירה (POS), בסיסי נתונים, שרתי אינטרנט וכיו"ב, וכן כל רכיבי תשלום חיוניים אחרים.*	
האם נעשה שימוש בסגמנטציית רשת המשפיעה על היקפה של סביבת ה-PCI DSS? (עיין בחלק "סגמנטציית רשת" של PCI DSS להנחיות בנוגע לסגמנטציה של הרשת הארגונית)	☐ כן ☐ לא

חלק 2ו: שירותי צד ג'

האם החברה משתפת את נתוני כרטיסי האשראי עם ספקים של שירותי צד ג' (לדוגמה, שירותי גישה לרשת, שירותי עיבוד תשלומים, ספקים של שירותי תשלום (PSP), חברות אירוח אתרים, סוכני הזמנת טיסות, סוכני תוכניות נאמנות וכיו"ב)?	☐ כן ☐ לא

אם כן:

שם ספק השירות:	תיאור השירות הניתן:

הערה: *דרישה 12.8 חלה על כל הישויות ברשימה זו.*

Copyright 2014 PCI Security Standards Council LLC

חלק 2ז: סיווג מתאים למילוי שאלון C	
בית העסק מאשר כי סיווגו מתאים למילוי גרסה מקוצרת זו של שאלון הערכה עצמית מהנימוקים הבאים:	
☐	לארגון שלך יש מערכת תשלום וחיבור לאינטרנט מאותו מכשיר/עמדה ו/או מאותה רשת מקומית (LAN);
☐	מערכת התשלום/המחשב המחובר לאינטרנט אינם מחוברים לאף מערכת אחרת בארגון;
☐	החנות של בית העסק אינה מחוברת לחניות במיקומים נוספים, וכל רשת מקומית (LAN) היא לחנות בודדת בלבד;
☐	בית העסק אינו מאחסן כלל נתונים של כרטיסי אשראי בפורמט אלקטרוני;
☐	אם בית העסק מחזיק בכל זאת נתוני כרטיסי אשראי, מידע זה מופיע אך ורק על דוחות וקבלות נייר ואינו מתקבל בצורה אלקטרונית.

Copyright 2014 PCI Security Standards Council LLC

פרק 2: שאלון הערכה עצמית C

הערה: *השאלות הבאות ממוספרות בהתאם לנהלי הבדיקה ולדרישות PCI DSS כפי שהוגדרו במסמך* דרישות ונהלי הערכת אבטחה של PCI DSS.

תאריך מילוי הטופס:

בנה ותחזק רשת בטוחה

דרישה 1: התקנה ותחזוקה של Firewall בתצורה המגנה על נתוני כרטיסי האשראי

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
1.2	האם קונפיגורצית ה – firewall והנתבים מגבילה את הגישה של רשתות לא אמינות לכל המערכות בסביבת נתוני כרטיסי האשראי כדלהלן: הערה: רשת לא אמינה הינה כל רשת חיצונית לרשתות השייכות לישות הנסקרת, ו/או מחוץ ליכולות השליטה או הניהול של הישות.						
1.2.1	א. האם התעבורה הנכנסת והיוצאת מוגבלת לזו ההכרחית לסביבת נתוני כרטיסי האשראי והאם הגבלות אלה מתועדות?	• עבור על הסטנדרטים של קונפיגורציות הנתב וה-firewall • בדוק את קונפיגורציות הנתב וה-firewall	☐	☐	☐	☐	☐
	ב. האם כל יתר התעבורה הנכנסת ויוצאת נחסמת באופן מפורש (למשל באמצעות חוק "deny all")?	• עבור על הסטנדרטים של קונפיגורציות הנתב וה-firewall • בדוק את קונפיגורציות הנתב וה-firewall	☐	☐	☐	☐	☐
1.2.3	האם הותקנו firewalls היקפיים בין כל הרשתות	• עבור על הסטנדרטים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	האלחוטיות וסביבת נתוני כרטיסי האשראי, והאם הוגדרו ה firewalls האלה לחסום כל תעבורה מהסביבה האלחוטית לסביבת נתוני כרטיסי האשראי או, אם תעבורה מסוג זה הכרחית לצורך עסקי, לאשר רק תעבורה מאושרת בין הסביבה האלחוטית לסביבת נתוני כרטיסי האשראי?	• בדוק את קונפיגורציות הנתב וה-firewall של					
1.3	האם הגדרות ה – firewall אוסרות על גישה ציבורית ישירה בין האינטרנט לבין כל רכיבי המערכת בסביבת נתוני כרטיסי האשראי באופן הבא:						
1.3.3	האם נאסרת תעבורה ישירה – נכנסת ויוצאת בין האינטרנט לבין סביבת נתוני כרטיסי האשראי?	• בדוק את קונפיגורציות הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.5	האם תעבורה היוצאת מסביבת נתוני כרטיסי האשראי לאינטרנט מאושרת באופן מפורש?	• בדוק את קונפיגורציות הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.6	האם מיושמת בדיקת עומק (stateful inspection) הידועה גם כסינון חבילות מידע דינאמי (dynamic packet filtering) (כלומר רק חיבורים "מוכרים" מורשים ברשת)?	• בדוק את קונפיגורציות הנתב וה-firewall	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

דרישה 2: אין להשתמש בהגדרות ברירת מחדל של ספקים עבור סיסמאות מערכת ומרכיבי אבטחה אחרים

	שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
2.1	א. האם ברירות מחדל המוגדרות על ידי הספק מוחלפות תמיד טרם התקנת המערכת ברשת? *נקודה זו מתייחסת לכל סיסמאות ברירות המחדל, כולל אבל לא מוגבל לסיסמאות בשימוש במערכות הפעלה, תוכנה המספקת שירותי אבטחה, יישום וחשבונות מערכת, מסופים בנקודות מכירה, SNMP, וכו'.*	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בחן את קונפיגורציית המערכת והגדרות החשבון • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם חשבונות ברירת מחדל לא נחוצים הוסרו או נוטרלו לפני התקנת מערכת על הרשת?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בחן את קונפיגורציית המערכת והגדרות החשבון • ראיין את כוח האדם	☐	☐	☐	☐	☐
2.1.1	האם בסביבות אלחוטיות המחוברות לסביבת נתוני כרטיסי אשראי, או המשדרות נתוני כרטיסים, כל ברירות המחדל האלחוטיות של הספק מוחלפות בעת ההתקנה באופן הבא:						
	א. האם מפתחות ההצפנה מוחלפים מברירת המחדל בזמן ההתקנה ובכל פעם שמישהו בעל ידע על המפתחות עוזב את החברה או מחליף תפקיד?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם מוחלפת הגדרת ברירת המחדל של ה SNMP community strings	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	במכשירים אלחוטיים בזמן ההתקנה?	• בחן מסמכי ספקים • בחן את קונפיגורציית המערכת והגדרות החשבון • ראיין את כוח האדם					
ג.	האם הסיסמאות המוגדרות כברירת מחדל בכל נקודות הגישה מוחלפות בזמן התקנה?	• עבור על מדיניות והליכים • ראיין את כוח האדם • בדוק את קונפיגורציות המערכת	☐	☐	☐	☐	☐
ד.	האם רכיב התוכנה בתוך החומרה של המכשיר האלחוטי מעודכן על מנת לתמוך בהצפנה חזקה לצורך זיהוי ושידור מעל רשתות אלחוטיות?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בדוק את קונפיגורציות המערכת	☐	☐	☐	☐	☐
ה.	האם ברירות מחדל אחרות המוגדרות על ידי הספק מוחלפות כשצריך?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בדוק את קונפיגורציות המערכת	☐	☐	☐	☐	☐
2.2 א.	האם נקבעו נהלים להגדרת תצורה לכל רכיבי המערכת והאם הם תואמים לסטנדרטים המקובלים בתעשייה בנוגע להקשחת מערכות? *מקורות לסטנדרטים מקובלים בתעשייה להקשחת מערכות כוללים בין היתר אבל לא רק את, SysAdmin Audit Network (SANS), National*	• עבור על סטנדרטים קונפיגורציית הרשת • עבור על הסטנדרטים המקובלים בתעשייה להקשחת מערכות • עבור על מדיניות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
Institute of Standards Technology (NIST), International Organization for Standardization (ISO), Center of Internet Security (CIS).	והליכים • ראיין את כוח האדם					
ב. האם הסטנדרטים להגדרת תצורת המערכת מתעדכנים כאשר מתגלות נקודות תורפה חדשות כמוגדר בדרישה 6.1?	• עבור על מדיניות והליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
ג. האם פועלים על פי הסטנדרטים להגדרת תצורת מערכת כאשר מוגדרת מערכת חדשה?	• עבור על מדיניות והליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
ד. האם הסטנדרטים להגדרת תצורת מערכת כוללים את הדברים הבאים: • החלפת כל ברירות המחדל המסופקות על ידי הספק והסרת כל חשבונות ברירת המחדל המיותרים? • יישום פעולה מרכזית אחת בלבד בכל שרת כדי למנוע מצב בו פעולות הדורשות רמת אבטחה שונה נמצאות יחד על אותו שרת? • מתן אישור רק לשירותים, פרוטוקולים, דיימונים, וכו' כפי הנדרש לתפקוד המערכת? • יישום מאפייני אבטחה נוספים עבור שירותים, פרוטוקולים או דיימונים נצרכים הנחשבים בלתי-מאובטחים? • תצורת פרמטרים של אבטחת המערכת כדי	• עבור על הסטנדרטים של קונפיגורציות המערכת					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	למנוע שימוש לא ראוי? • הסרת תפעולים לא הכרחיים כגון תוכנות script, כוננים, מאפיינים, תתי-מערכות, מערכות קבצים, ושרתי רשת לא נחוצים?						
2.2.1	א. האם ישנו ייעוד שימוש עיקרי אחד לכל שרת על מנת למנוע מצב בו ייעודי שימוש שונים הדורשים רמת אבטחה שונה מתקיימים על אותו שרת? (לדוגמה, שרתי web, שרתי database, ושרתי DNS צריכים להיות מוקמים על שרתים נפרדים).	• בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ב. אם נעשה שימוש בטכנולוגיית וירטואליזציה, האם ישנו ייעוד שימוש עיקרי אחד לכל רכיב או מערכת וירטואלית?	• בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
2.2.2	א. האם מאופשרת הפעילות רק של אותם שירותים, פרוטוקולים ודיימונים חיוניים באופן הנדרש לפעולתה של המערכת. (שירותים ופרוטוקולים שאינם נדרשים באופן ישיר על מנת לאפשר את פעולת המערכת מנוטרלים)?	• עבור על סטנדרטים של הקונפיגורציה • בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ב. האם השימוש בכל השירותים, פרוטוקולים ודיימונים הלא בטוחים אשר פועלים, מוצדק ומיושמים לפי הסטנדרטים של הקונפיגורציה המתועדת?	• עבור על הסטנדרטים של הקונפיגורציה • ראיין את כוח האדם • בחן את הגדרות הקונפיגורציה • השווה בין שירותים וכן הלאה מאושרים לבין הצדקות מתועדות	☐	☐	☐	☐	☐
2.2.3	האם מאפייני אבטחה נוספים מתועדים ומיושמים עבור כל שירות,	• עבור על הסטנדרטים של					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	פרוטוקול או דיימון נחוצים הנחשבים ללא-בטוחים? (לדוגמה, טכנולוגיות אבטחה כמו SSH, FTP-S, SSL, IPSec או VPN מיושמות על מנת להגן על שירותים לא בטוחים כגון NetBios, שיתוף קבצים, Telnet, FTP וכו).	הקונפיגורציה • בחן את הגדרות הקונפיגורציה					
2.2.4	א. האם אדמיניסטרטור המערכת או האנשים האחראיים על קביעת תצורת רכיבי המערכת, הנם בעלי ידע בפרמטרים הנפוצים של הגדרת אבטחת המערכת?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם הפרמטרים הנפוצים של הגדרת תצורת אבטחת המערכת כלולים בסטנדרטים של תצורת המערכת?	• בחן את הסטנדרטים של קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ג. האם הפרמטרים של הגדרת תצורת אבטחת המערכת, מיושמים כהלכה על כל רכיבי המערכת?	• בחן את מרכיבי המערכת • בחן את הגדרות פרמטר האבטחה • השווה את ההגדרות לסטנדרטים של קונפיגורציית המערכת	☐	☐	☐	☐	☐
2.2.5	א. האם כל היישומים הלא הכרחיים כגון – סקריפטים, דרייברים, תכונות, תתי מערכות, מערכות קבצים ושרתי Web, הוסרו?	• בחן את פרמטרים האבטחה על מרכיבי המערכת	☐	☐	☐	☐	☐
	ב. האם היישומים הפועלים מתועדים והאם הם פועלים בתצורה מאובטחת?	• עבור על המסמכים • בחן את פרמטרים האבטחה על מרכיבי המערכת	☐	☐	☐	☐	☐
	ג. האם רק יישומים מתועדים קיימים ברכיבי המערכת?	• עבור על המסמכים בחן את פרמטרים האבטחה על מרכיבי	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		המערכת					
2.3	האם גישת אדמיניסטרטור שלא דרך מסוף (non console admin access) מוצפנת כדלהלן: *השתמש בטכנולוגיות כגון SSH, VPN או TLS/SSL בשימוש בגישה ניהולית דרך האינטרנט או כאשר נעשה שימוש בממשקי גישה אדמיניסטרטיביים שלא דרך מסוף אחרים.*						
א.	האם כל גישת אדמיניסטרטור שלא דרך מסוף, מוצפנת באמצעות מנגנון הצפנה חזק, והאם ההצפנה מופעלת לפני שהאדמיניסטרטור מתבקש לספק את הסיסמה?	• בחן את רכיבי המערכת • בחן את קונפיגורציית המערכת • צפה במנהל נכנס למערכת	☐	☐	☐	☐	☐
ב.	האם תצורת שירותי המערכת וקבצי פרמטרים נקבעה באופן שימנע שימוש ב Telnet או באמצעים לא בטוחים אחרים לגישה מרחוק?	• בחן את רכיבי המערכת • בחן שירותים וקבצים	☐	☐	☐	☐	☐
ג.	האם גישת אדמיניסטרטור מהאינטרנט לממשקי ניהול מוצפנת באמצעות מנגנון הצפנה חזק?	• בחן את רכיבי המערכת • צפה במנהל נכנס למערכת	☐	☐	☐	☐	☐
ד.	עבור הטכנולוגיה שבשימוש, האם מנגנון הצפנה חזק מיושם בהתאם לנהלים הטובים במשק (best practice) ו/או המלצות הספק?	• בחן את רכיבי המערכת • בחן את מסמכי הספקים • ראיין את כוח האדם					
2.5	האם מדיניות האבטחה ונהלי הפעולה לניהול ברירות מחדל של הספק ופרמטרים אחרים של אבטחה:	• עבור על מדיניות האבטחה ונהלי הפעולה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
• מתועדים • בשימוש ידועים לכל הצדדים הרלוונטיים?	• ראיין את כוח האדם					

Copyright 2014 PCI Security Standards Council LLC

הגנה על נתוני אשראי

דרישה 3: הגן על הנתונים המאוחסנים של כרטיסי האשראי

	שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
3.2	ג. האם מידע אימות רגיש מושמד או אינו ניתן לשחזור לאחר השלמת הליך האימות?	• עבור על המדיניות וההליכים • בחן את הקונפיגורציה של המערכת • בחן את דרישות השמירה	☐	☐	☐	☐	☐
	ד. האם כל המערכות עונות לדרישות הבאות בנוגע לאי-שמירה של מידע אימות רגיש לאחר אישור עסקה (אפילו אם הוא מוצפן)?						
3.2.1	האם תכולתו המלאה של אף אחד מהערוצים (track) מהפס המגנטי (הממוקם בגב הכרטיס, או מידע זהה הממוקם על שבב או בכל מקום אחר) אינה נשמרת לאחר אימות? *מידע זה גם נקרא ערוץ מלא (full track), ערוץ 1 (track 1), ערוץ 2 (track 2) ופרטי הפס המגנטי.* *הערה: ייתכן ובמהלכם הרגיל של העסקים יהיה צורך לשמור את הפרטים הבאים המצויים בפס המגנטי:* ▪ *שם בעל הכרטיס* ▪ *מספר כרטיס האשראי (PAN)* ▪ *תאריך התפוגה (תוקף)* ▪ *וקוד השירות* *על מנת לצמצם את הסיכון, שמור רק את הפרטים הללו כאשר יש צורך עסקי בכך.*	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐
3.2.2	האם הקוד (CVC) או ערך הקוד (CVV) לאימות הכרטיס (המספר בעל שלוש או ארבע ספרות המודפס בקדמת או בגב הכרטיס) אינו נשמר לאחר	• בחן מקורות מידע כולל: • מידע נכנס על	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	האימות?	עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע					
3.2.3	האם מספר הזיהוי האישי (PIN) או בלוק מידע הכולל את ה PIN המוצפן אינם נשמרים לאחר האימות?	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐
3.3	האם מספר כרטיס האשראי ממוסך כאשר הוא מוצג (שש הספרות הראשונות וארבע הספרות האחרונות הן המספר המקסימלי של ספרות שיוצגו) כך שרק עובדים עם צורך עסקי לגיטימי יוכלו לראות את ה-PAN המלא? *הערה: דרישה זו אינה גוברת על דרישות מחמירות יותר הנוגעות להצגה של נתוני מחזיקי כרטיסי אשראי – למשל דרישות סוג כרטיס תשלום או דרישות משפטיות בנוגע לקבלות בנקודות מכירה (POS).*	• עבור על המדיניות והנהלים • עבור על התפקידים שצריכים גישה לתצוגה מלאה של ה-PAN • בחן את קונפיגורציית המערכת • צפה בתצוגות של PAN	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

דרישה 4: הצפן את השידור של נתוני כרטיסי אשראי על פני רשתות ציבוריות פתוחות

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
4.1	א. האם נעשה שימוש בהצפנה חזקה ובפרוטוקולי אבטחה כגון TLS/SSL, SSH, IPSEC על מנת להגן על נתונים רגישים של כרטיסי אשראי במהלך שידור על פני רשתות ציבוריות פתוחות? *דוגמאות לרשתות ציבוריות פתוחות הרלוונטיות להקשר של תקן PCI DSS כוללות אך לא מוגבלות ל: אינטרנט; טכנולוגיות אלחוטיות כולל 802.11 ובלוטות'; טכנולוגיות סלולריות, כגון GSM, CDMA ו GPRS*	• עבור על סטנדרטים מתועדים • עבור על מדיניות והליכים • עבור על כל המקומות בהם CHD משודר או נקלט • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ב. האם מתקבלים רק מפתחות ו/או אישורים ממקור בטוח?	• צפה בתשדורות פנימה והחוצה • בחן מפתחות ואישורים	☐	☐	☐	☐	☐
	ג. האם פרוטוקולי האבטחה מיושמים אך ורק בתצורה מאובטחת ולא תומכים בגרסאות תצורה לא מאובטחות?	• בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ד. האם מיושם חוזק הצפנה המתאים לשיטת ההצפנה שנעשה בה שימוש (בדוק את המלצות הספק/סטנדרטים מקובלים)?	• בחן את מסמכי הספקים • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ה. ליישומי TLS/SSL, האם SSL/TLS מאופשר כאשר נתוני מחזיקי כרטיסי אשראי	• בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
משודרים או מתקבלים? *לדוגמה, עבור יישומים מבוססי דפדפן:* • *האם בדפדפן מופיע HTTPS כחלק מכתובת האינטרנט (URL)?* • *האם נתוני כרטיסי אשראי נדרשים רק כאשר מופיע HTTPS בכתובת האינטרנט בדפדפן (URL)?*							
האם נעשה שימוש בנהלים מקובלים בתעשייה (למשל, IEEE 802 11i), כדי ליישם הצפנה חזקה של תהליכי אימות ושידור עסקאות ברשתות אלחוטיות שמשדרות נתוני כרטיסי אשראי או מחוברות לסביבת כרטיסי האשראי? ***הערה:*** *השימוש ב WEP כבקרת אבטחה אסור.*	4.1.1	• עבור על סטנדרטים מתועדים • עבור על רשתות אלחוטיות • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
ב.האם ישנם נהלים הקובעים כי אין לשלוח מספרי כרטיסי אשראי בלתי מוגנים באמצעות טכנולוגיות העברת מסרים של משתמשי קצה?	4.2	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

יישם ותחזק תוכנית לניהול נקודות תורפה

דרישה 5: הגן על כל המערכות נגד תוכנות זדוניות ועדכן את תוכנת האנטי וירוס באופן קבוע

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
5.1	האם מותקנת תוכנת אנטי וירוס על כל המערכות שבדרך כלל מושפעות/עשויות להיפגע מתוכנות זדוניות?	• בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
5.1.1	האם כל תוכנות האנטי-וירוס המותקנות מסוגלות לזהות, להסיר ולהגן מפני כל הסוגים הידועים של תוכנות זדוניות (לדוגמה, וירוסים, סוסים טרויאנים, תולעים, תוכנות ריגול, תוכנות פרסומת, וערכות ריגול (rootkit))?	• בחן את מסמכי הספקים • בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
5.1.2	האם מתבצעות הערכות תקופתיות כדי לזהות ולהעריך איומים מתפתחים של תוכנות זדוניות על מנת לאשר שהמערכות שנחשבות כלא מושפעות מתוכנות זדוניות נשארות כאלו?	• ראיין את כוח האדם					
5.2	האם כל תוכנות האנטי וירוס מעודכנות, פועלות ומייצרות לוגים לבקרה (audit logs) כדלקמן:						
	א. האם נוהל האנטי-וירוס דורש עדכון של תוכנת האנטי-וירוס וההגדרות שלה?	• עבור על מדיניות והליכים • בחן את קונפיגורציי ת אנטי-וירוס, כולל את ההתקנה הראשית • בחן את רכיבי המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
ב.	האם עדכונים אוטומטים וסריקות תקופתיות מוגדרים כפעילים?	• בחן את קונפיגורציי ת אנטי-וירוס, כולל את ההתקנה הראשית • בחן את רכיבי המערכת	☐	☐	☐	☐	☐
ג.	האם כל מנגנוני האנטי וירוס מייצרים לוגים לבקרה (Audit logs) והאם הלוגים נשמרים בהתאם לדרישה 10.7 לתקן PCI DSS?	• בחן את קונפיגורציות האנטי-וירוס • עבור על הלוגים של הליכי שימור	☐	☐	☐	☐	☐
5.3	האם כל המנגנונים נגד וירוסים: • פעילים? • בלתי ניתנים לכיבוי או שינוי על ידי המשתמשים? ***הערה:*** *ניתן לכבות זמנית פתרונות אנטי-וירוס רק במקרה של צורך טכנולוגי, כפי שמאושר על ידי ההנהלה על בסיס כל מקרה לגופו. אם יש צורך לבטל את הגנת האנטי-וירוס למטרה ספציפית, חייב להיות אישור רשמי. יתכן ויהיה צורך באמצעי אבטחה נוספים בזמן שהגנת האנטי-וירוס לא פעילה.*	• בחן את קונפיגורציות האנטי-וירוס • בחן את רכיבי המערכת • צפה בהליכים • ראיין את כוח האדם					

Copyright 2014 PCI Security Standards Council LLC

דרישה 6: פתח ותחזק מערכות ואפליקציות מאובטחות

	שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
6.1	האם ישנו תהליך שנועד לזהות נקודות תורפה באבטחה כולל: • שימוש במקורות חיצוניים אמינים עבור מידע על נקודות תורפה? • דירוג רמת סיכון לנקודות תורפה הכולל זיהוי כל נקודות התורפה בעלות סיכון "גבוה" ו-"קריטי"? ***הערה**: דירוג הסיכונים צריך להיות מבוסס על סטנדרטים מקובלים בתעשייה כמו גם על התחשבות בהשפעה פוטנציאלית. לדוגמה, קריטריונים לדירוג נקודות תורפה יכולים לכלול הסתמכות על הציון הבסיסי ב- CVSS ו/סיווג על ידי הספק ו/או סוג המערכות שיושפעו.* *שיטות להערכת נקודות תורפה ודירוג הסיכונים ישתנו בהתאם לסביבת הארגון ואסטרטגיית הערכת הסיכונים שלו. לכל הפחות, הערכת סיכונים צריכה לזהות את כל נקודות התורפה הנחשבות לבעלות "סיכון גבוה" לסביבה. בנוסף לדירוג הסיכון, נקודות תורפה יכולות להיחשב "קריטיות" אם הן מהוות איום מיידי לסביבה, משפיעות על מערכות קריטיות, ו/או יגרמו לבעיית אבטחה פוטנציאלית אם לא יוטפלו. דוגמאות למערכות קריטיות כוללות מערכות אבטחה, מכשירים ומערכות הנמצאים בקשר עם הציבור, מאגרי מידע ומערכות אחרות המאחסנות, מעבדות או משדרות נתוני מחזיקי כרטיסי אשראי.*	• עבור על מדיניות והליכים • ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
6.2	א. האם כל רכיבי המערכת והתוכנה מוגנים מפני חשיפה לנקודת תורפה ידועות באמצעות התקנה של טלאי האבטחה (patches)	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	המעודכנים ביותר של הספק?						
ב.	האם טלאי האבטחה (patches) מותקנים בתוך חודש אחד מיום פרסומם? ***הערה:*** *יש לזהות טלאי אבטחה קריטיים לפי תהליך דירוג רמת סיכון המתואר בדרישה 6.1*	• עבור על מדיניות והליכים • בחן רכיבי מערכת • השווה בין רשימת טלאי האבטחה המותקנים לבין רשימות הטלאים העדכניות	☐	☐	☐	☐	☐

הטמע אמצעי בקרת גישה חזקים

דרישה 7: הגבל את הגישה לפרטי כרטיסי האשראי עפ"י העקרון של הצורך העסקי לדעת

שאלה		דרישות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
7.1	האם הגישה לרכיבי מערכת ולנתוני כרטיסי אשראי מוגבלת רק לאנשים שתפקידם מחייב זאת, כדלקמן:						
7.1.2	האם הקצאת ההרשאות המיוחדות לעובדים המורשים מוגבלת כדלקמן?	• ראיין את כוח האדם • ראיין את	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		דרישות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
• למספר ההרשאות המינימלי הדרוש למילוי התפקיד? • הקצאה רק לתפקידים שדורשים גישה מסווגת זו?		• ההנהלה • עבור על מספרי משתמש מסווגים					
האם גישה מאושרת בהתבסס על הסיווג והתפקוד של כל תפקיד?	7.1.3	• ראיין את ההנהלה • עבור על מספרי המשתמש	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

דרישה 8: זהה ואשר גישה לרכיבי מערכת

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
8.1.5	א. האם חשבונות המשמשים ספקים לגישה, תמיכה או תחזוקה של רכיבי המערכת דרך גישה מרחוק מאופשרים רק למשך הזמן הדרוש ומנוטרלים כאשר הם לא בשימוש?	• עבור על תהליכי סיסמאות • ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
	ב. האם חשבונות ספקים בגישה מרחוק מנוטרים כאשר הם בשימוש?	• ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
8.3	האם שילוב של שני גורמי אימות (Two-Factor Authentication) מיושם עבור גישה מרחוק (גישה ברמת הרשת ממקום הנמצא מחוץ לרשת) של עובדים, מנהלי מערכת וגורמים אחרים (כולל גישת ספקים עבור תמיכה או תחזוקה)?). ***הערה:*** *אימות כפול דורש ששתיים מתוך שלוש שיטות האימות (ר' דרישה 8.2 לתיאור שיטות האימות) ישמשו לאימות. שימוש באותה שיטה פעמיים (למשל שימוש בשתי סיסמאות נפרדות) אינו נחשב אימות כפול.* *דוגמאות לאימות כפול כוללות שירות חיוג ואימות מרחוק (RADIUS) עם tokens או בקרת גישה באמצעות מסוף Access Controller Access Control System (TACACS) עם tokens; או טכנולוגיות אחרות*	• עבור על מדיניות והליכים • בחן את קונפיגורציית המערכת • צפה בעובדים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
המיישמות אימות כפול.						

דרישה 9: הגבל את הגישה הפיזית לנתונים של כרטיסי אשראי

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
9.1.2	האם הגישה הפיזית לשקעי רשת שיש אליהם נגישות ציבורית מוגבלת? *לדוגמה, שקעי רשת לא יימצאו באזורים שיש בהם גישה לאורחים, אלא אם הגישה לרשת הותרה במפורש*. לחילופין, יש ליישם הליכים לוודא שיש תמיד ליווי של אורחים באזורים בהם יש חיבורי רשת פעילים.	• עבור על מדיניות והליכים • ראיין את כוח האדם • צפה במקומות	☐	☐	☐	☐	☐
9.5	האם כל סוגי המדיה, מאובטחים פיזית (לרבות, אך לא רק, מחשבים, אמצעי אחסון אלקטרוניים ניידים, קבלות נייר, דוחות נייר ופקסים)? *למטרות דרישה 9, המונח "מדיה" מתייחס לכל הניירת ואמצעי האחסון האלקטרוניים המכילים נתוני כרטיסי האשראי.*	• עבור על מדיניות והליכים לאבטחה פיזית של מדיה • ראיין את כוח האדם	☐	☐	☐	☐	☐
9.6	א. האם קיימת בקרה מחמירה על התפוצה הפנימית והחיצונית של כל סוגי המדיה?	• עבור על מדיניות והליכים לסיווג מדיה • ראיין עובדי	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		אבטחה					
	ב. האם הבקרות כוללות את הדברים הבאים:						
9.6.1	האם המדיות מסווגות כך שניתן לזהות מהי רמת הרגישות של המידע (המצוי בהן)?	• ראיין את כוח האדם • בחן את יומני הפצת המדיה והתיעוד	☐	☐	☐	☐	☐
9.6.2	האם המדיות נשלחות באמצעות שליח מאובטח או בשיטת מסירה אחרת המאפשרת לעקוב אחריהן באופן מדויק?	• ראיין את כוח האדם • בחן את יומני הפצת המדיה והתיעוד	☐	☐	☐	☐	☐
9.6.3	האם נדרש אישור הנהלה לפני העברה של מדיות (במיוחד כשהן מופצות ליחידים)?	• ראיין את כוח האדם • בחן את יומני הפצת המדיה והתיעוד	☐	☐	☐	☐	☐
9.7	האם ישנה בקרה מחמירה על אופן האחסון והנגישות למדיות (המכילות נתוני כרטיסי אשראי)?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
9.8	א. האם כל המדיות המכילות נתוני כרטיסי אשראי מושמדות כאשר אין בהן עוד צורך עסקי או חוקי?	• עבור על מדיניות והליכים להשמדת מדיה תקופתית	☐	☐	☐	☐	☐
	ג. האם המדיה מושמדת בצורה הבאה:						
9.8.1	א. האם מדיה קשיחה נגרסת, נשרפת או נכתשת באופן שאינו מאפשר לשחזר את	• ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	הנתונים של כרטיסי האשראי? ?	• בחן הליכים • צפה בהליכים					
	ב. האם מכלים המאחסנים מידע המיועד להשמדה מאובטחים באופן המונע גישה לתכולתם?	• בחן אבטחה של המכלים המאחסנים מידע	☐	☐	☐	☐	☐
9.9	האם מכשירים המאחסנים נתוני כרטיסי אשראי דרך ממשק פיזי עם הכרטיס מוגנים נגד החלפה והתעסקות ? ***הערה:*** *דרישה זו מתייחסת למכשירי קריאת כרטיסים המשמשים בעסקאות בהם הכרטיס נוכח פיזית (יש העברת כרטיס פיזית) בנקודת המכירה. דרישהזו לא מתייחסת לרכיבים של הקלדה ידנית כגון על מקלדות מחשבים או POS.* ***הערה:*** *דרישה 9.9 מהווה המלצה עד ל-30 ביוני, 2015, ולאחר מכן תהפוך לדרישה.*						
	א. האם המדיניות וההליכים מחייבים שמירת רשימה של מכשירים כאלו?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
	ב. האם המדיניות וההליכים מחייבים בדיקה תקופתית של מכשירים אלו לגילוי התערבות או החלפה?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
	ג. האם המדיניות וההליכים מחייבים הכשרה של העובדים לעירנות להתנהגות חשודה ולדיווח התערבות או החלפה של המכשירים?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
9.9.1	א. האם רשימת	• בחן את	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	המכשירים כוללת את הנתונים הבאים? • סוג, מודל המכשיר. • מיקום המכשיר (לדוגמה, כתובת האתר או המתקן בו נמצא המכשיר) • מספר סידרתי של המכשיר או שיטת זיהוי ייחודית אחרת	רשימת המכשירים					
ב.	האם הרשימה מדויקת ומעודכנת?	• צפה במיקום המכשירים והשווה לרשימה	☐	☐	☐	☐	☐
ג.	האם רשימת המכשירים מעודכנת כאשר מכשירים מתווספים, משנים מיקום, יוצאים מכלל פעולה, ועוד?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
9.9.2 א.	האם משטחי המכשירים נבדקים תקופתית כדי לגלות התערבות (לדוגמה, הוספה של קוראי כרטיסים למכשיר) או החלפה (לדוגמה, על ידי בדיקת המספר הסידרתי או מאפייני מכשיר אחרים לוודא שהמכשיר לא הוחלף בזיוף) כדלקמן: ***הערה:*** *דוגמאות לסימנים של התעסקות או החלפה של מכשיר כוללים תוספות לא צפויות או כבלים המחוברים למכשיר, תוויות אבטחה חסרות או שונות, כיסוי שבור או בצבע שונה, או שינויים במספר הסידרתי או סימנים חיצוניים אחרים.*	• ראיין את כוח האדם • צפה בהליכי הבדיקה והשווה להליכים המוגדרים	☐	☐	☐	☐	☐
ב.	האם העובדים	• ראיין את	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מודעים להליכים לבדיקת המכשירים?	כוח האדם					
9.9.3	האם העובדים מקבלים הכשרה כדי להיות ערנים לאפשרות של מכשירים שהוחלפו או התעסקו איתם, כולל הבאים:						
א.	• האם חומרי ההכשרה עבור עובדים בנקודות מכירה כוללים את הנקודות הבאות? • אימות זיהוי של אנשים מצד שלישי הטוענים שהם עובדי תחזוקה או שירות לפני שהם מקבלים גישה לשנות או לתקן מכשירים • אין להתקין, להחליף, או להשיב מכשירים ללא אימות • יש לשים לב להתנהגות חשודה סביב מכשירים (לדוגמה, ניסיונות של אנשים לא ידועים לפתוח מכשירים או לנתקם) • יש לדווח לעובדים המתאימים (כגון מנהל או קצין אבטחה) על התנהגות חשודה וסימנים של התעסקות או החלפה של המכשיר.	• עבור על חומר ההכשרה	☐	☐	☐	☐	☐
ב.	• האם העובדים בנקודות המכירה קיבלו הכשרה, והם מודעים להליכים לגילוי ודיווח ניסיונות להתעסק עם המכשירים או להחליפם?	• ראיין עובדים בנקודות המכירה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

בצע ניטור ובדיקה של הרשת באופן קבוע

דרישה 10: נטר ועקוב אחר כל גישה למשאבי הרשת ולנתוני כרטיסי האשראי

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
10.2	האם מיושם נתיב ביקורת (audit trails) אוטומטי עבור כל רכיבי המערכת על מנת שניתן יהיה לשחזר את האירועים הבאים:						
10.2.2	כל הפעולות שבוצעו על ידי משתמש יחיד בעל הרשאות ניהול או הרשאות root?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.4	ניסיונות בלתי תקפים לקבלת גישה לוגית?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.5	שימוש במנגנוני הזיהוי והאימות - כולל אבל לא מוגבל ליצירת חשבונות חדשים והגברת הרשאות - וכל השינויים, התוספות או ההסרות לחשבונות עם הרשאות root ניהוליות?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3	האם השדות הבאים מופעים מופיעים בנתיב הביקורת (audit trail) של המערכת בעת התרחשות של כל אירוע (event) של						

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
המערכת?						
10.3.1 זהות המשתמש?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.2 סוג האירוע (event)?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.3 תאריך ושעה?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.4 סימון הצלחה או כישלון?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.5 מקור היווצרות האירוע?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		הביקורת					
10.3.6	זהותם או שמם של הנתונים, רכיבי המערכת או המשאבים המושפעים?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.6	האם הלוג היומנים וכל אירועי האבטחה של כל רכיבי המערכת נסקרים חריגים כדי לזהות פעילות חריגה או חשודה כדלקמן: ? *__הערה__: ניתן להשתמש בטכנולוגיות כגון כלי איסוף, ניתוח והתראה של לוגים על מנת לעמוד בדרישה 10.6*						
10.6.1	ב. האם היומנים ואירועי האבטחה לעיל מבוקרים לפחות פעם ביום?	• צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
10.6.2	ב. האם סקירות של כל מרכיבי המערכת האחרים מבוצעות בהתאם לאסטרטגיית ניהול הסיכונים והמדיניות של הארגון?	• עבור על מסמכי ניהול סיכון • ראיין את כוח האדם	☐	☐	☐	☐	☐
10.6.3	ב. בהתאם בוצע מעקב אחר חריגים ויוצאי-דופן?	• צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
10.7	ב. האם קבצי לוג ביקורת (audit logs) זמינים למשך שנה לפחות?	• ראיין את כוח האדם • בחן יומני	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ביקורת					
ג. האם הלוגים של שלושת החודשים האחרונים לפחות זמינים מיידית לצרכי ניתוח?	• ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

דרישה 11: בצע בדיקות שוטפות של מערכות ותהליכי האבטחה

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
11.1	א. האם יש תהליכים מיושמים לגילוי וזיהוי של נקודות גישה אלחוטיות מורשות ובלתי מורשות על בסיס רבעוני? ***הערה**: השיטות שבהן ניתן לעשות שימוש בתהליך זה כוללות, אך אינן מוגבלות לאמצעים הבאים: סריקה של רשתות אלחוטיות, בדיקות פיזיות/לוגיות של רכיבי מערכת ותשתית, בקרת גישת רשת (NAC) או פריסת IDS/IPS אלחוטי.* *יהיו אשר יהיו השיטות שבהן נעשה שימוש, עליהן להיות מספיקות לאיתור וזיהוי של כל התקן בלתי מורשה.*	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
	ב. האם השיטה לגילוי וזיהוי של נקודות גישה אלחוטיות לא מורשות כוללת גילוי וזיהוי של הרכיבים הבאים לכל הפחות: • כרטיס רשת אלחוטית (WLAN) שהוכנסו לרכיבי מערכת; • מכשירים אלחוטיים ניידים שחוברו לרכיבי מערכת כדי ליצור נקודת גישה אלחוטית (למשל, באמצעות USB,	• הערך את השיטה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	וכו) ; • מכשיר אלחוטי המחובר לערוץ (port) רשת או למכשיר ברשת?						
	ג. האם התהליך לזיהוי נקודות גישה אלחוטיות מורשות ובלתי מורשות מבוצע על כל רכיבי המערכת והמתקנים בכל האתרים ולפחות פעם ברבעון?	• בחן פלט מסקירות אלחוטיות אחרונות	☐	☐	☐	☐	☐
	ד. האם מיושם ניטור אוטומטי (למשל, IPS/IDS אלחוטי, NAC, וכו'), האם הניטור מוגדר לייצר התראות לעובדים?	• בחן הגדרות קונפיגורציה	☐	☐	☐	☐	☐
11.1.1	האם יש מלאי של נקודות גישה אלחוטית מורשות עם תיעוד של סיבות עסקיות עבור כל נקודות הגישה האלחוטית המורשות? ?	• בחן רשומות מלאי	☐	☐	☐	☐	☐
11.1.2	א. האם התוכנית לתגובה לאירוע מגדירה ומצריכה תגובה במקרה ונמצאה נקודת גישה אלחוטית בלתי מורשת?	• בחן תוכנית תגובה לאירוע (ראה דרישה 12.10)	☐	☐	☐	☐	☐
	ב. האם ננקטת פעולה כאשר מתגלית נקודת גישה אלחוטית בלתי מורשית?	• ראיין את העובדים האחראים • בדוק סקירות אלחוטיות אחרונות ותגובות קשורות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
11.2	האם סריקות פנימיות וחיצוניות לאיתור פרצות רשת מורצות לפחות אחת לרבעון ולאחר כל שינוי משמעותי ברשת (התקנת רכיבי מערכת חדשים, שינויים בטופולוגית הרשת, שינויים בחוקי ה-firewall שדרוגים של מוצרים) באופן הבא? ***הערה**: אפשר לאחד דוחות סקירה מרובים עבור הליך הסקירה הרבעוני כדי להראות שכל המערכות נסרקו וכל נקודות התורפה הרלוונטיות טופלו. ייתכן וידרשו מסמכים נוספים כדי לוודא שיגיעו גם לנקודות תורפה שלא טופלו* *אין חובה שארבע סריקות רבעוניות עם תוצאה עוברת יושלמו לקראת תאימות <u>ראשונית</u> עם תקן PCI DSS אם 1) הסריקה האחרונה היתה בעלת תוצאה עוברת, 2) הישות תעדה מדיניות ונהלים הדורשים סריקה רבעונית, ו 3) נקודות התורפה שנמצאו בסריקה ומופיעות בדוח הסריקה תוקנו כפי שמוכיחה סריקה החוזרת. עבור תאימות לתקן בשנים שאחרי הסקירה הראשונית של PCI, יש חובה לבצע 4 סריקות רבעוניות עם תוצאה עוברת.*						
11.2.1	א. האם מתבצעות סריקות פנימיות למציאת נקודות תורפה אחת לרבעון?	• עבור על דוחות סקירה	☐	☐	☐	☐	☐
	ב. האם תהליך הסריקה הפנימית הרבעוני כולל סריקות חוזרות עד אשר מתקבלת תוצאה עוברת או עד אשר כל נקודות התורפה המדורגות ברמת סיכון "גבוהה"	• עבור על דוחות סקירה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	כמוגדר בדרישה 6.1 של PCI DSS, טופלו?						
	ג. האם הסריקות הפנימיות הרבעוניות מבוצעות על ידי כח אדם פנימי או חיצוני מיומן, וכאשר רלוונטי, האם מתקיים עקרון אי התלות של הבודק בארגון (לא חייב להיות QSA או ASV)?	• עבור על דוחות סקירה	☐	☐	☐	☐	☐
11.2.2	א. האם מבוצעות סריקות רבעוניות חיצוניות למציאת נקודות תורפה? ***הערה:*** *סקירות חיצוניות רבעוניות חייבות להיות מבוצעות על ידי ספק סקירה מאושר (ASV) המאושר על ידי ה- PCI SSC.* *ראה במדריך ה-ASV המפורסם באתר PCI SSC עבור אחריות הלקוח לסריקה, הכנות לסריקה ועוד*	• עבור על התוצאות מארבעת הרבעונים האחרונים של סקירה חיצונית למציאת נקודות תורפה	☐	☐	☐	☐	☐
	ב. האם הסריקות החיצוניות הרבעוניות מקיימות את דרישות תכנית ההדרכה של ASV (למשל, לא צריכות להימצא בסריקה נקודות תורפה המדורגות גבוה יותר מ 4.0 על פי דירוג ה CVSS ולא כישלונות אוטומטיים)?	• עבור על התוצאות של כל סקירה רבעונית חיצונית וסקירה מחדש	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ג. האם הסריקות הרבעוניות החיצוניות מבוצעות על ידי ספק סריקה מאושר (ASV), אשר אושר על ידי מועצת ה PCI (PCI SSC)?	• עבור על התוצאות של כל סקירה רבעונית חיצונית וסקירה מחדש	☐	☐	☐	☐	☐
11.2.3	א. האם סריקות פנימיות וחיצוניות וסריקות מחדש מבוצעות לאחר כל שינוי מהותי? ***הערה**: הסריקות חייבות להתבצע על ידי כח אדם מיומן.*	• בחן ותאם מסמכים על בקרת שינויים ודוחות סקירה	☐	☐	☐	☐	☐
	ב. האם תהליך הסריקה כולל סריקות חוזרות עד אשר: • עבור סריקות חיצוניות – אין נקודות תורפה קיימות אשר קיבלו ציון גבוה מ 4.0 על פי דירוג ה CVSS • עבור סריקות פנימיות – התקבלה תוצאה עוברת או לחילופין כל נקודות התורפה המדורגות ברמת סיכון "גבוהה" טופלו בהתאם	• עבור על דוחות הסקירה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
למוגדר בדרישה 6.1 ל PCI DSS.						
ג. האם הסריקות מבוצעות על ידי כח אדם פנימי או חיצוני מיומן, וכאשר רלוונטי, האם מתקיים עקרון אי התלות של הבודק בארגון (לא חייב להיות QSA או ASV)?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
11.3.4 אם יש שימוש בסגמנטציה כדי לבודד את ה-CDE מרשתות אחרות: א. האם תהליכים לבדיקת חדירות מוגדרים לבדיקת כל שיטות הסגמנטציה, לאשר שהן פעילות ויעילות ולבודד את כל המערכות שמחוץ להיקף מהמערכות שבהיקף?	• בחן בקרת סגמנטציה • עבור על שיטת בדיקת חדירות					
ב. האם בדיקות החדירה לוודא ביקורת סגמנטציה עונות על התנאים הבאים: • מבוצעות לפחות פעם בשנה ולאחר שינויים בשיטת/ בקרת הסגמנטציה • מכסות את כל שיטות/ בקרת הסגמנטציה שבשימוש • מוודאות ששיטות	• בחן תוצאות מבדיקת החדירה האחרונה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	הסגמנטציה פעילות ויעילות ומבודדות את כל המערכות שמחוץ להיקף מהמערכות שבהיקף						
11.5	א. האם מיושם מנגנון לגילוי שינוי (לדוגמה כלים לניטור שלמות קבצים (file integrity)) בסביבת נתוני כרטיסי האשראי כדי לגלות שינויים בלתי מורשים בקבצי מערכת חיוניים, קבצי קונפיגורציה, או קבצי תוכן? *דוגמאות לסוגי קבצים שצריכים להיות מנוטרים:* • *קבצי מערכת הניתנים להרצה (executables)* • *קבצי אפליקציה הניתנים להרצה (executables)* • *קבצי פרמטרים וקבצי קונפיגורציה* • *קבצי לוג וביקורת הנשמרים בצורה מרוכזת, בהיסטוריה או בארכיב* • *קבצים חיוניים נוספים הנקבעים על ידי אחראי (כגון דרך הערכת סיכונים או*	• צפה בהגדרות המערכת וקבצים מנוטרים • בחן את הגדרות קונפיגורציית המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
בדרכים נוספות)							
ב.	האם הכלים מוגדרים לשלוח התרעות לגורמים הרלוונטיים על כל שינוי לא מורשה של קבצי מערכת קריטיים, קבצי קונפיגורציה או קבצי תוכן, והאם הכלים מבצעים השוואות קבצים קריטיים לפחות פעם בשבוע? ***הערה**: לצורך ניטור שלמות הקבצים – קבצים קריטיים הם אלו שבדרך כלל אינם עוברים שינויים תכופים, אך שינויים בהם עשויים להצביע על פגיעה במערכת או חשש לפגיעה. כלי ניטור שלמות קבצים מגיעים בדרך כלל עם הגדרות מוכנות מראש עבור קבצים קריטיים במערכת ההפעלה הרלוונטית. קבצים קריטיים אחרים, כגון קבצים לאפליקציות שפותחו פנימית, צריכים לעבור הערכה והגדרה על ידי הישות (כלומר בית העסק או ספק השירות).*	• צפה בהגדרות המערכת וקבצים מנוטרים • עבור על התוצאות מפעילות הניטור	☐	☐	☐	☐	☐
11.5.1	האם יש תהליך להגבה על התראות המיוצרות על ידי פתרון גילוי שינוי?	• בחן את הגדרות קונפיגורציי ת המערכת					

Copyright 2014 PCI Security Standards Council LLC

יישם ותחזק מדיניות אבטחת מידע

דרישה 12: יישם ותחזק מדיניות הנותנת מענה לאבטחת מידע בקרב כלל כח האדם (עובדים וקבלנים)

הערה: *לצרכי כוונת סעיף 12, "כח האדם" מתייחס לעובדים במשרה מלאה, עובדים במשרה חלקית, עובדים זמניים, קבלנים וייועצים שעובדים פיזית בתוך מתחמי הארגון או לחילופין שיש להם גישה לסביבת נתוני כרטיסי האשראי של החברה.*

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
12.1	האם מדיניות האבטחה קיימת, מפורסמת, מתוחזקת ומופצת לכל כח האדם הרלוונטי?	▪ עבור על מדיניות אבטחת המידע	☐	☐	☐	☐	☐
12.1.1	האם מדיניות אבטחת המידע נסקרת/נבדקת לפחות אחת לשנה ומעודכנת בהתאם לצורך על מנת לשקף שינויים ביעדי העסק ובסביבת הסיכונים שלו?	▪ עבור על מדיניות אבטחת המידע ▪ ראיין עובדים אחראיים	☐	☐	☐	☐	☐
12.3	האם פותחה מדיניות שימוש בטכנולוגיות קריטיות על מנת להבטיח את השימוש הנאות בטכנולוגיות הללו ואשר כוללת את הדרישות הבאות: ***הערה:*** *טכנולוגיות קריטיות כוללות לדוגמה, אבל לא רק, טכנולוגיות גישה מרחוק, טכנולוגיות אלחוטיות, מדיות אלקטרוניות נשלפות, מחשבים ניידים, טבלטים, מחשבי כף יד, דוא"ל ואינטרנט*						
12.3.1	אישור מפורש מטעם גורמים מורשים לשימוש בטכנולוגיות?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.2	אימות המשתמש עבור השימוש	▪ עקוב אחר	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	בטכנולוגיה?	מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים					
12.3.3	רשימה של המכשירים מסוג זה והעובדים בעלי הגישה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.4	תיוג המכשירים לזיהוי הבעלים, פרטי ההתקשרות וייעוד המכשיר?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.5	שימושים מקובלים בטכנולוגיה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.6	מיקומי רשת מקובלים עבור הטכנולוגיות?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.8	ניתוק אוטומטי של חיבורי גישה מרחוק לאחר פרק זמן מוגדר של חוסר פעילות?	▪ עקוב אחר מדיניות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		▪ שימוש ▪ ראיין מדגם של עובדים אחראיים					
12.3.9	הפעלת טכנולוגיות גישה מרחוק עבור יצרנים ושותפים עסקיים רק כשהיצרנים והשותפים העסקיים זקוקים לגישה כזאת וסגירתה מיד בתום השימוש?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.4	האם המדיניות ונהלי האבטחה מגדירים בבירור את תחומי האחריות של כל עובד בכל הקשור לאבטחת מידע?	▪ עבור על מדיניות והליכים של אבטחת מידע ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.5	ב. האם סמכויות הניהול הבאות בתחום אבטחת המידע מוקצות לאדם או לקבוצה:						
12.5.3	פיתוח, תיעוד והפצת נהלי תגובה לאירועי אבטחה ותהליכי הסלמה (אסקלציה) על מנת להבטיח טיפול יעיל ומתוזמן היטב בכל מצבי האבטחה?	▪ עבור על מדיניות והליכים של אבטחת מידע	☐	☐	☐	☐	☐
12.6	א. האם ישנה תכנית מודעות אבטחה רשמית שתפקידה לגרום לכלל העובדים להיות מודעים לחשיבות אבטחת נתוני כרטיסי אשראי?	▪ עבור על התוכנית למודעות לאבטחה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
12.8	אם נתוני כרטיסי האשראי מועברים לספקי שירות אחרים, האם קיימים ומוטמעים מדיניות ונהלים לניהול ספקי השירות, כדלהלן?						
12.8.1	האם ישנה רשימה מתוחזקת של ספקי השירות?	▪ עבור על מדיניות והליכים ▪ צפה בהליכים ▪ עבור על רשימת ספקי השירות	☐	☐	☐	☐	☐
12.8.2	האם קיים הסכם בכתב הכולל הכרה באחריותו של ספק השירות לאבטחת נתוני כרטיסי האשראי הנמצאים ברשותו או שהוא מאחסן, מעבד או משדר עבור הלקוח, או במידה שהם יכולים להשפיע על האבטחה של סביבת נתוני כרטיסי האשראי של הלקוח? ***הערה:*** *המינוח המדויק של ההכרה יהיה תלוי בהסכם בין שני הצדדים, פרטי השירות המסופק, והאחריות המוטלת על כל אחד מהצדדים. ההכרה לא חייבת לכלול את המינוח המדויק המופיע בדרישה זו.*	▪ צפה בהסכמים הכתובים ▪ עבור על מדיניות והליכים	☐	☐	☐	☐	☐
12.8.3	האם קיים תהליך מסודר להתחלת העסקה של ספק שירות, לרבות בדיקת נאותות הולמת לפני תחילת העבודה מולו?	▪ צפה בתהליכים ▪ עבור על מדיניות והליכים ומסמכים תומכים	☐	☐	☐	☐	☐
12.8.4	האם קיימת תכנית כדי לנטר אחר מצב התאימות של ספקי השירות לתקן PCI DSS לפחות פעם בשנה?	▪ צפה בתהליכים ▪ עבור על מדיניות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		והליכים ומסמכים תומכים					
12.8.5	האם נשמר מידע בנוגע לאילו דרישות PCI DSS מטופלות על ידי איזה ספק שירות, ואילו מטופלות על ידי הארגון?	▪ צפה בתהליכים ▪ עבור על מדיניות והליכים ומסמכים תומכים	☐	☐	☐	☐	☐
12.10.1	א. האם פותחה תכנית תגובה לאירוע אבטחה שניתן ליישמה במקרה של אירוע פריצת אבטחה במערכת?	▪ עבור על תוכנית תגובה לאירוע ▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
	ב. האם התכנית כוללת לכל הפחות:						
	▪ הקצאת תפקידים, תחומי אחריות, ואסטרטגיות תקשורת ויצירת קשר במקרה של סכנת אבטחה כולל עדכון חברות האשראי, לכל הפחות?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
	▪ נהלי תגובה מוגדרים וספציפיים לאירועי אבטחה?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
▪ נהלי התאוששות והמשכיות עסקית?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ תהליכי גיבוי מידע?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ ניתוח דרישות החוק בנוגע לדיווח על אירועי פרצות אבטחה?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ כיסוי ותגובה בנוגע לכל רכיבי המערכת הקריטיים?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ הפנייה או והטמעה של נהלי התגובה של חברות המותג של כרטיסי האשראי לאירועי אבטחה?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

נספח א': דרישות נוספות עבור ספקי אירוח משותף (Shared Hosting Providers)

נספח זה אינו לשימוש הערכת בתי עסק.

Copyright 2014 PCI Security Standards Council LLC

נספח ב': גיליון בקרות מפצות

יש להשתמש בגיליון עבודה זה כדי להגדיר את הבקרות המפצות עבור כל אחת מן הדרישות אשר סומנה עבורה התשובה " כן עם גליות עבודה של בקרות מפצות".

הערה: *רק חברות שביצעו הערכת סיכונים ושיש להן אילוצים עסקיים או טכנולוגיים מתועדים לגיטימיים רשאיות לעשות שימוש בבקרות מפצות על מנת לעמוד בתקן.*

עיין בנספחים B,C ו- D של מסמך PCI DSS לקבלת מידע על בקרות מפצות והדרכה כיצד להשלים גיליון זה.

מספר הדרישה והגדרתה:

	מידע נדרש	הסבר
1. אילוצים	מנה את האילוצים המונעים עמידה בדרישת התקן המקורית.	
2. יעד	הגדר את יעד הבקרה המקורית ; זהה את היעד המושג על ידי הבקרה המפצה.	
3. הסיכון המזוהה	זהה סיכונים נוספים הנובעים מהעדרו של אמצעי הבקרה המקורי.	
4. הגדרה הבקרה המפצה	הגדר את הבקרות המפצות והסבר כיצד הן נותנות מענה ליעדי הבקרה המקורית והסיכון המוגבר, אם קיים.	
5. בדיקת תקפות הבקרה המפצה	הגדר כיצד נבדקו הבקרות המפצות וכיצד אושררה תקפותן.	
6. תחזוקה	הגדר את התהליכים ואמצעי הבקרה המיושמים לצורך תחזוקת הבקרות המפצות.	

Copyright 2014 PCI Security Standards Council LLC

נספח ג': הסבר על חוסר רלוונטיות (N/A)

במידה והוזן ערך "N/A" או "לא רלוונטי", יש להשתמש בגיליון עבודה זה כדי להסביר מדוע הדרישה האמורה אינה רלוונטית לארגון.

דרישה	הסיבה לחוסר הרלוונטיות
דוגמה: *3.4*	*נתוני כרטיסי האשראי אף פעם לא מאוחסנים באופן אלקטרוני.*

Copyright 2010 PCI Security Standards Council LLC

פרק 3 – אישור ואימות פרטים

חלק 3. אישור PCI DSS

בהסתמך על התוצאות שהתקבלו בשאלון C מתאריך *(תאריך מילוי השאלון)*, *(שם נותן שירות)* מצהיר על סטטוס התאימות הבא (יש לסמן אחד):

☐ **עומד בתקן**: כל חלקי שאלון PCI SAQ מולאו וכל השאלות נענו בחיוב ולפיכך הדירוג הכללי של החברה הוא **עומד בתקן**, **ובנוסף** סריקה עם ציון עובר בוצעה על ידי ספק סריקות מאושר (ASV) בהתאם לכך *(שם נותן שירות)* הראה תאימות מלאה לדרישות PCI DSS.

☐ **לא עומד בתקן:** לא מולאו כל חלקי שאלון PCI SAQ, או שישנן שאלות שהתשובה אליהן היתה "לא", ולכן דירוגה הכללי של החברה **לא עומד בתקן**, **או** לא בוצעה סריקה עם ציון עובר על ידי ספק סריקות מאושר (ASV), לפיכך *(שם נותן שירות)* לא הראה תאימות מלאה לדרישות PCI DSS.

- **תאריך יעד** לתאימות לתקן:
- ישות עסקית המגישה טופס זה עם סטטוס 'לא עומד בתקן' עשויה להידרש לביצוע 'תוכנית הפעולה' המפורטת בחלק 4 שבמסמך זה. *יש לברר מול חברת כרטיסי האשראי או מותג(י) האשראי שאיתו(ם) אתם עובדים לפני ביצוע חלק 4 הואיל ולא כל חברות מותגי האשראי דורשות חלק זה.*

☐ **עומד בתקן אבל עם החרגה משפטית:** אחד או יותר מהדרישות סומנו "לא" בשל מגבלה משפטית המונעת מהדרישה להתקיים. אפשרות זו מחייבת בחינה נוספת של חברת האשראי. אם אופציה זו סומנה, השלם את הטבלה הבאה:

דרישה רלוונטית	פירוט כיצד מגבלה משפטית מונעת מהדרישה להתקיים

חלק 3א. אישור סטטוס התאימות

נותן השירות מאשר כי:

☐	שאלון הערכה עצמית C של PCI DSS, גרסה (מס' הגרסה של השאלון), הושלם בהתאם להוראות המופיעות בו.
☐	כל המידע הנכלל בשאלון האמור ובהצהרה זאת מייצג נאמנה את תוצאות ההערכה שלי בכל ההיבטים המהותיים.
☐	אישרתי עם ספק התשלומים שלי כי מערכת התשלומים אינה מאחסנת נתוני אימות רגישים לאחר קבלת אישור.
☐	קראתי את תקנות PCI DSS ואני מכיר בזאת כי מחובתי לשמור על תאימות מלאה ל-PCI DSS בכל זמן.
☐	אם הסביבה שלי משתנה, אני מכיר בך שאני חייב להעריך מחדש את הסביבה שלי וליישם את כל

Copyright 2010 PCI Security Standards Council LLC

	דרישות PCI DSS נוספות שחלות.
☐	לא נמצאו כל ראיות לשמירה של נתוני הפס המגנטי[1], נתוני CAV2, CVC2, CID, או CVV2 [2], או נתוני PIN [3], לאחר אישור עסקה **באף אחת** מהמערכות שנבדקו במהלך הערכה זו.
☐	סריקות ASV הושלמו ומתבצעות על ידי ספר סריקה PCI DSS מאושר (שם ספק סקירה).

חלק 3ב. אישור נותן השירות	
חתימה של מנהל בכיר בבית העסק ↑	*תאריך* ↑
שם המנהל הבכיר בבית העסק ↑	*תפקיד* ↑

חלק 3ג. אישור QSA (אם רלוונטי)	
אם QSA היה מעורב או סייע בהערכה זו, תאר את התפקיד שבוצע:	
חתימה של נציג QSA: ↑	*תאריך* ↑
שם נציג QSA:	*חברת QSA:*

חלק 3ד. אישור ISA (אם רלוונטי)	
אם ISA היה מעורב או סייע בהערכה זו, תאר את התפקיד שבוצע:	
חתימה של נציג ISA: ↑	*תאריך* ↑
שם נציג ISA:	*תפקיד:*

[1] נתונים המקודדים בפס המגנטי או מידע דומה על שבב המשמשים לאישור בעסקאות בהן הכרטיס נוכח. יישויות אינן רשאיות לשמור את נתוני הפס המגנטי במלואם לאחר אישור העסקה. הערכים היחידים המצויים על הפס המגנטי ומותרים לשמירה הינם מספר הכרטיס, תאריך תפוגה, ושם בעל הכרטיס.

[2] המספר בעל שלוש או ארבע הספרות המודפס על תיבת החתימה או מימין לתיבת החתימה או על חזית הכרטיס האשראי המשמש לביצוע אימות בעסקאות בהן הכרטיס אינו נוכח.

[3] הקוד הסודי האישי המוקלד על ידי בעל הכרטיס בעסקאות בהן הכרטיס נוכח, ו/או מספר PIN מוצפן בהודעת העסקה.

Copyright 2010 PCI Security Standards Council LLC

חלק 4. תוכנית פעולה לסטטוס 'לא עומד בתקן'

אנא בחר את "סטטוס התאימות" המתאים לכל דרישה. אם התשובה לאחת מן הדרישות היא "**לא**", הנך נדרש למלא את התאריך שבו תעמוד החברה בדרישה ולתאר בקצרה את הפעולות הננקטות על מנת לעמוד בדרישה. *בדוק מול חברת כרטיסי האשראי או מותגי) האשראי לפני מילוי חלק 4, הואיל ולא כל חברות מותגי האשראי דורשות חלק זה.*

דרישת PCI DSS	תיאור הדרישה	סטטוס תאימות (בחר אחד)		תאריך ופעולות תיקון (אם סטטוס התאימות שסומן הוא "לא")
		כן	לא	
1	התקן ותחזק Firewall בתצורה המגנה על נתוני כרטיסי האשראי.	☐	☐	
2	אין להשתמש בהגדרות ברירת מחדל של ספקים עבור סיסמאות מערכת ומרכיבי אבטחה אחרים.	☐	☐	
3	הגן על הנתונים המאוחסנים של כרטיסי האשראי.	☐	☐	
4	הצפן את ההעברה של פרטי בעל הכרטיס על פני רשתות ציבוריות פתוחות.	☐	☐	
5	הגן על כל המערכות נגד תוכנות זדוניות ועדכן את תוכנת האנטי וירוס באופן קבוע.	☐	☐	
6	פתח ותחזק מערכות ואפליקציות מאובטחות.	☐	☐	
7	הגבל את הגישה לפרטי כרטיסי האשראי עפ"י העקרון של הצורך העסקי לדעת.	☐	☐	
8	זהה ואשר גישה לרכיבי מערכת.	☐	☐	
9	הגבל את הגישה הפיזית לנתונים של כרטיסי האשראי.	☐	☐	
10	נטר ועקוב אחר כל גישה למשאבי הרשת ולנתוני כרטיסי האשראי.	☐	☐	
11	בצע בדיקות שוטפות של מערכות ותהליכי האבטחה.	☐	☐	
12	יישם ותחזק מדיניות המטפלת באבטחת מידע בקרב כלל כח האדם (עובדים וקבלנים).	☐	☐	

Copyright 2010 PCI Security Standards Council LLC